IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1. (Currently Amended) A method and means for the secure notification of data subjects in privacy environments defined by directive, law or contract, ~~of secure privacy notification in accordance with regulatory compliance requirements~~, said method and means comprising the steps:

~~determining said regulatory compliance~~ applying legal and contractual requirements for privacy notification of data subjects;

transforming said requirements into ~~electronic and non-electronic~~ database field query screens and forms ~~for viewing by a user~~;

querying a ~~remote and/or resident~~ database for privacy protected information fields contained within said query screens and forms;

~~said data screens being adapted for~~ human and/or automated completion of said data screens;

encryption/decryption of said data screens;

~~said data screens being adapted for~~ human and/or automated conversion of said data screens into privacy notification human readable formats;

data subject feedback response methods and means; and

conversion of said data subjects feedback responses into database controller notification for deletion, modification or correction of the data subject's information in accordance with said ~~regulatory~~ requirements.

2. (Originally Presented) The method of claim 1 wherein said electronic privacy notification and feedback response is accomplished via a secure web portal.

3. (Originally Presented) The method of claim 1 wherein said electronic privacy notification and feedback response is accomplished via a secure e-mail system.

4. (Previously Presented) The method of claim 1 wherein said electronic privacy notification and feedback response is accomplished using digital certificates comprising:

a public or private, commercial or government registration authority;

a public or private, commercial or government certificate authority;

a digital signature encryption algorithm;

a unique non-reputable user electronic identity;

issuance of x.509 compliant certificates specifically encoded via extension to alert data processor of the data subjects privacy preferences; and

issuance of x.509 standard certificates specifically encoded via extension to alert data processors of legal and regulatory compliance requirements relevant to the data subjects privacy preferences.

5. (Originally Presented) The method of claim 4 wherein said digital signature algorithm is SHA-1 with DSA.

6. (Originally Presented) The method of claim 4 wherein said digital signature algorithm is an elliptic curve.

7. (Originally Presented) The method of claim 6 wherein said elliptic curve is a Koblitz binary curve.

8. (Originally Presented) The method of claim 4 wherein said digital signature algorithm is a block cipher such as Rijndael.

9. (Originally Presented) The method of claim 4 wherein the data subjects privacy preference is to "opt out" and where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

10. (Originally Presented) The method of claim 4 wherein the data subjects privacy preference is to "opt in" and where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

11. (Originally Presented) The method of claim 4 including third party archiving of certificate for non-repudiation, compliance audit and send and receive functions.

12. (Currently Amended) The method in claim 4 including the binding of a user's identity and access authorizations to a physical device, such as a USB key, and challenging the key at a remote email server in order to gain access to the users authorized email box and messages.

13. (Currently Amended) An apparatus for protection of privacy and required notification of data subjects in accordance with ~~regulatory~~ compliance requirements, said apparatus comprising:

a determining device for determining said ~~regulatory~~ compliance requirements for said privacy and required notification of data subjects;

a transforming device for transforming said compliance requirements into data field query screens;

~~an~~ a query device for querying a database for information fields contained within said query screens;

a completion device to facilitate completion and processing of said query screens with said information field;

an encryption device for non-repudiated encryption of the data obtained from said completed query screens;

a decryption device for non-repudiated decryption and conversion of the data obtained from the completed query screens into compliant privacy notification of said data subjects in a human readable formats;

a notification feedback device for providing data subject notification feedback; and

a conversion device for conversion of said data subjects feedback response into correction, modification or deletion of the data subject's information in accordance with said regulatory requirements.

14. (Previously Presented) The apparatus of claim 13 further including a USB key that contains encryption and processing circuitry, authorized user bound identity information and volatile and/or non-volatile memory that stores the algorithms used to query for said data fields.

15. (Previously Presented) The apparatus of claim 13 further including a hardware firewall that contains encryption and processing circuitry, authorized user bound identity information and volatile and/or non- volatile memory that stores the algorithms used to query said data fields.

16. (Previously Presented) The apparatus of claim 13 further including a software firewall that contains encryption and processing instruction sets, authorized user bound identity information and volatile and/or non-volatile memory that stores the algorithms used to query said data fields.

17. (Previously Presented) The apparatus of claim 13, wherein said privacy regulatory compliance requirements are derived from the laws, rules and regulations promulgated by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

18. Cancelled

19. (Previously Presented) The apparatus of claim 13, wherein the privacy regulatory compliance requirements are derived from the laws, rules and regulations promulgated by The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

20. Cancelled

21. Cancelled

22. (Previously Presented) The apparatus of claim 13, wherein said electronic privacy notification and feedback response is accomplished via a secure socket layer web portal.

23. (Previously Presented) The apparatus of claim 13, wherein said electronic privacy notification and feedback response is accomplished via a secure e-mail system.

24. (Previously Presented) The apparatus of claim 13, where wherein said privacy notification and feedback response is accomplished via postal notification.

25. Cancelled

26. Cancelled

27. (Previously Presented) The method of claim 4, including the binding of a user's identity and access authorizations to a physical device, such as a USB

key, and challenging the key at a remote email server or secure web portal in order to gain access to the users authorized email or web messages.

28. (Previously Presented) The method in claim 4 including the binding of a user's identity and access authorizations to software tokens and challenging the tokens at a remote email server or secure web portal in order to gain access to the users authorized email or web messages.